Unleashing the power of innovative aerospace technology....

@Columns

Air Force Research Laboratory AFRL

news@afrl

April - June 1999 **Official voice of the Air Force Research Laboratory**

CIO Topics

Meeting the challenges of Y2K

We are at the welcome mat of the new millennium and are facing a troublesome problem that some say threatens to cripple existing technology. The Air Force Research Laboratory is carefully planning for the new century and working to meet system and software challenges that may result from the Year 2000 "bug," also known as the Y2K problem.

The Y2K problem is a result of programming practices from the early days of computers involving the use of six-digit dates, dd/mm/yy, versus eight-digit dates, dd/mm/yyyy. This results in the possibility of a date such as "11/11/31" being interpreted by a computer as November 11, 1931, instead of November 11, 2031. Any computer program that deals with six-digit dates may be susceptible to the Y2K problem.

Another problem involved in the Y2K issue is date mathematics. For years, businesses have used this method to track things such as aging schedules, due dates, past due accounts, etc. Many applications now use date mathematics. These applications use a base year, often January 1, 1900, as the starting point for tracking date and time.

For example, a computer program would calculate the difference between January 1, 1998, and January 1, 1999, as 365 days. Calculating the difference between today and when a bill was incurred would tell you how old a bill was (i.e., 30 days). Since computers usually use the six-digit date system, a situation like 12/08/99 through 01/01/00 might be misinterpreted by the computer system as December 8, 1999, through January 1, 1900. The calculation would result in a large negative number (in the tens of thousands). This may or may not be a problem that the computer program can deal with.

It is possible that this resulting number would also be made into an absolute value, which drops the negative sign if no space is reserved to hold it, causing even more confusion. Imagine if your debt went from 23 days old to 36,114 days!

The second type of Y2K problem involves systems that check to determine if a valid date is used. For example, a security system may check to see if today's date is valid before recording an entry or exit from the building. If the "00" date is determined to be out of range, i.e. occurred 100 years ago, the system would shut down and lock the doors.

Our lab-wide Y2K program has been recognized as one of the best in the Air Force and Department of Defense. Every computer resource and piece of software nestled deep inside AFRL systems has been assessed for compliance. Only 13 percent of AFRL's hardware and software remain non-compliant. We are continuing to eliminate problems with non-compliant technologies daily by installing the appropriate "fixes" that will ensure these systems continue to work without problems when we step off the welcome mat and into the next century.

One of three things will happen to items that are found non-compliant:

1. They will be fixed – updated chips installed or software patches applied once the vendors make the solutions available;
2. They will be replaced – new items will be bought, or;
3. They will be reset – the system clock can be reset after January 1, 2000, and the system will continue to operate as before. @

Info about INFOCON

In the wake of virus attacks by "Melissa," "Happy '99," etc., it is important to recognize that while people once went off to war, modern science can bring it to our doorstep.

In the event that you receive a virus message, contact your Computer Systems Security Officer or your systems administrator.

In response to this new threat, Information Operations Conditions have been established for AFRL. The INFOCON recommends actions to uniformly heighten or reduce our defensive posture, to defend against computer network attacks and to buffer the harmful effects of sustained damage to the DOD information infrastructure (computer and telecommunication networks and systems).

Each INFOCON level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are Normal (day-to-day activity), Alpha (increased risk of attack), Bravo (specific risk of attack), Charlie (limited attack), and Delta (general attack). Each level has a list of preventative actions, actions to be taken during an actual attack, and damage control/mitigating actions.

Your Information Technology staff will distribute a list of actions to take when confronted with these INFOCON levels. Though prematurely linking actual actions to levels is classified, we are currently at INFOCON BRAVO.